NAHOEMI PABLO

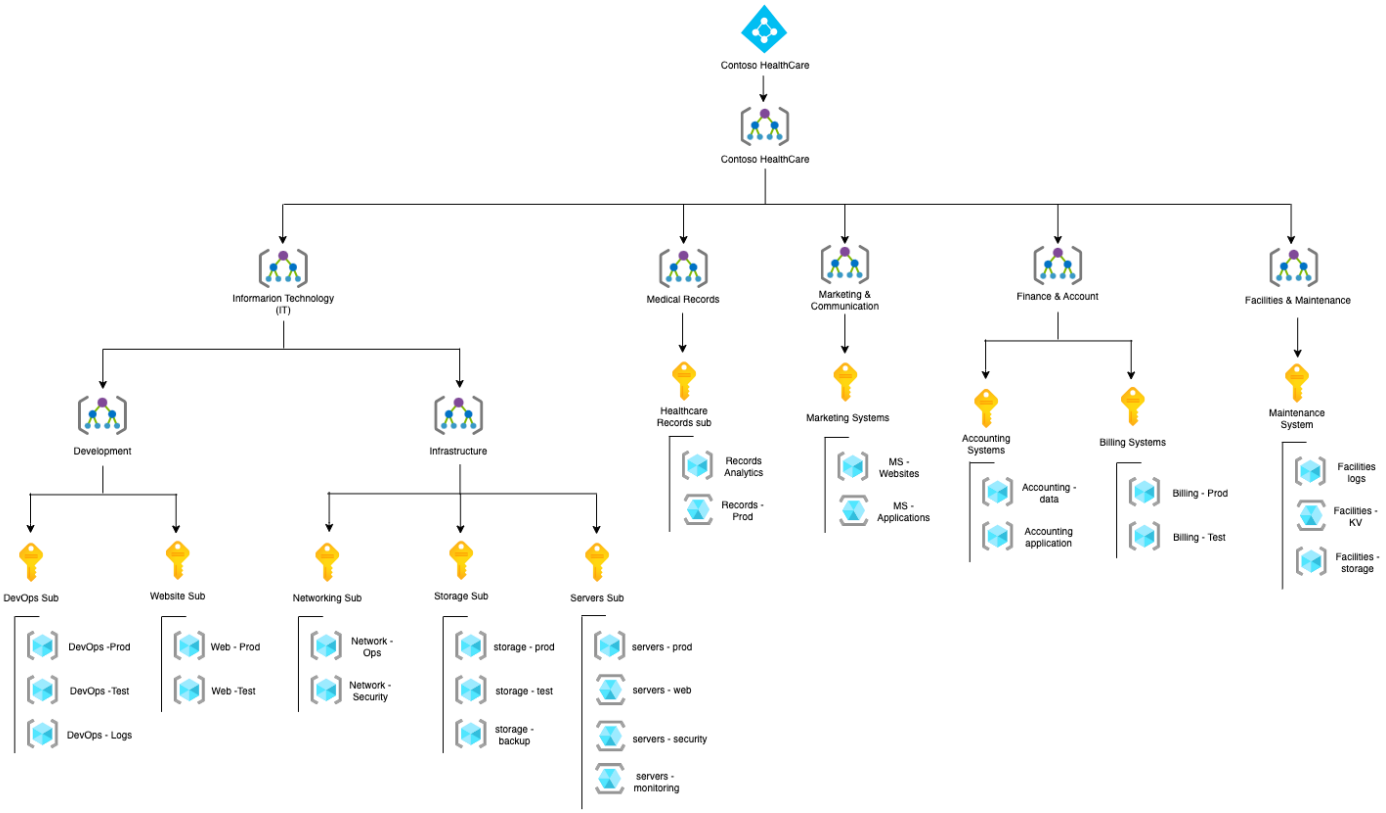
Project: Implementing Secure Cloud Governance at “Contoso Healthcare”

In this project (scale down model), I navigated a real-world scenario assuming the role of an Azure identity engineer in a healthcare organization, “Contoso Healthcare.” The organization is in the process of transitioning into Azure cloud, and it is crucial to establish proper identity and access management along with governance controls in the Azure environment.

As the lead identity engineer on Contoso Healthcare cloud migration project, I was responsible for designing and implementing identity management, access controls, and governance processes for the new Azure environment.

- Lead the deployment and configuration of the Azure AD by integrating identities into Azure cloud.
- Implement Azure role-based access controls (RBAC) by granting least privilege based on job roles and responsibilities.
- Develop and enforce security policies on user accounts, data, and resources within the environment.
- Set up actionable budget alerts and utilization reporting.
- Implement self-service password reset for employees within the organization.

Azure Management Group Diagram



To effectively execute this project; the implementation will be structured across four key phases:

Part 1: Configure the Azure AD tenant by establishing users, groups, licensing, and self-service password reset capabilities.

Part 2: Implement Azure role-based access controls (RBAC) by creating roles with appropriate permissions to Azure resource groups. Assign permissions to users and/or groups at the appropriate scopes to grant least privilege access.

Part 3: Deploying governance tools such as Azure Policy, resource locks, and tags in the environment.

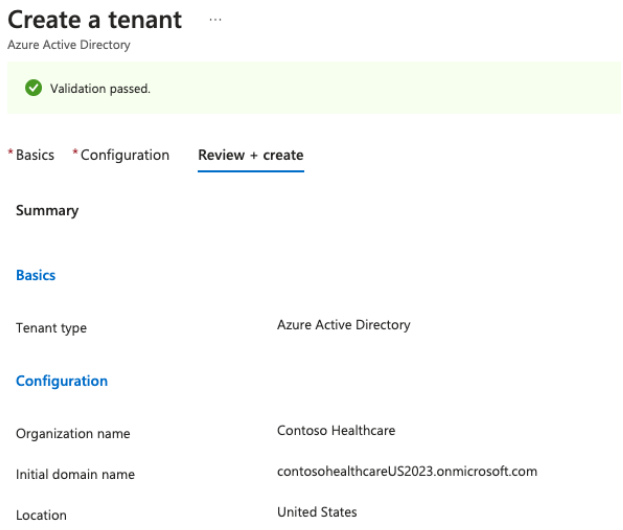
Part 4: Optimize cost management through budgets, and alerts.

Let's get started!

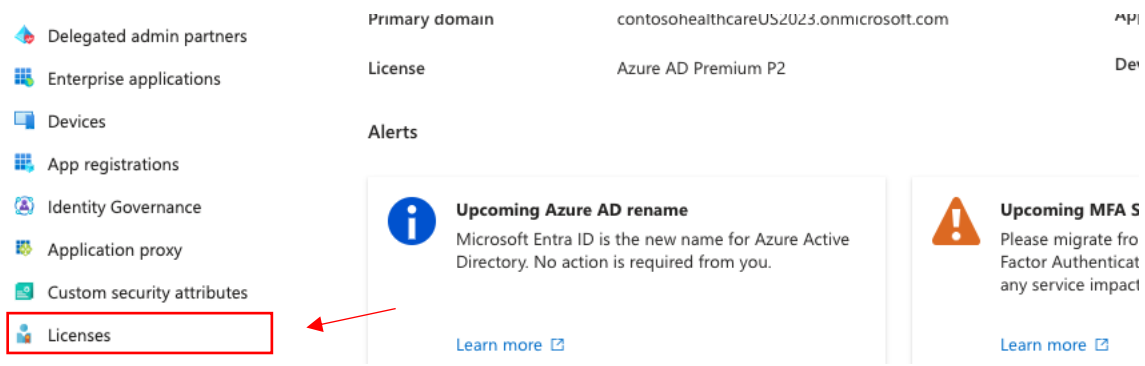
Part 1: Configure the Azure AD tenant by establishing users, groups, licensing, and self-service password reset capabilities.

The focus of part one is to concentrates on deploying Azure Active Directory as the primary identity and access management provider by creating user accounts, security groups, licensing, and self-service password reset. This forms the identity foundation for assigning permissions in later phases.

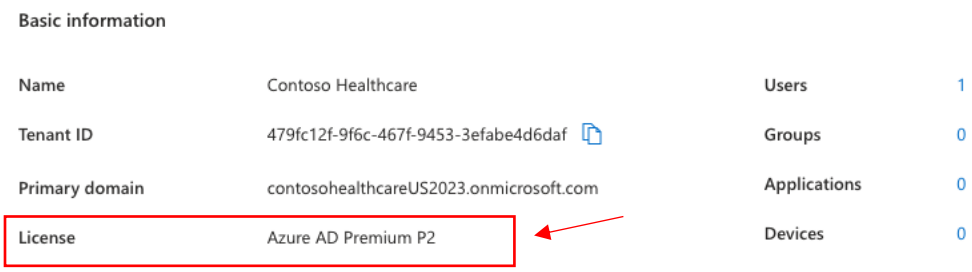
Step 1: Select "**Create a resource**" and search for "**Azure Active Directory**." Select "**Create**" and fill out the tenant configuration with Contoso Healthcare information. After filling out the information select "**Create.**" After these steps, we have successfully created an Azure Tenant for Contoso Healthcare Azure Active Directory.



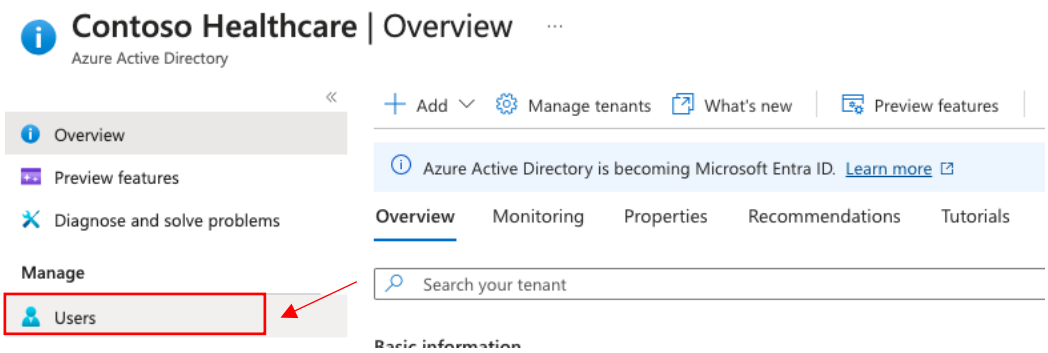
Step 2: Under *Contoso Healthcare Overview*, select "**Licenses"** and apply the appropriate license for this project which is Azure AD Premium P2.



After applying the correct license to Contoso Healthcare, the next step is to refresh Contoso Healthcare | Overview page to see the Azure AD Premium P2 license.

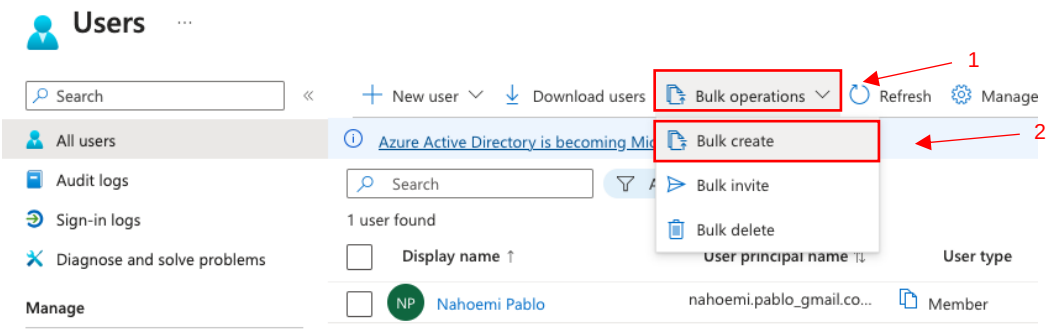


Step 3: In the *Azure Portal*, locate and select "**Azure Active Directory**" from the left-hand navigation pane. Under *manage*, select "**Users**" to access user management page.



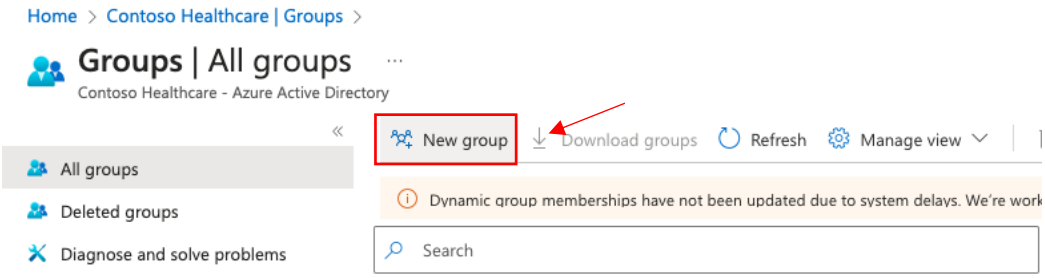
Note: For this project, I will select the "**Bulk Operations**" to create all the users simultaneously.

Step 3: Select "**Bulk Operations"** follow by "**Bulk Create"** and upload your csv file with the employee's first name, last name, job title etc.



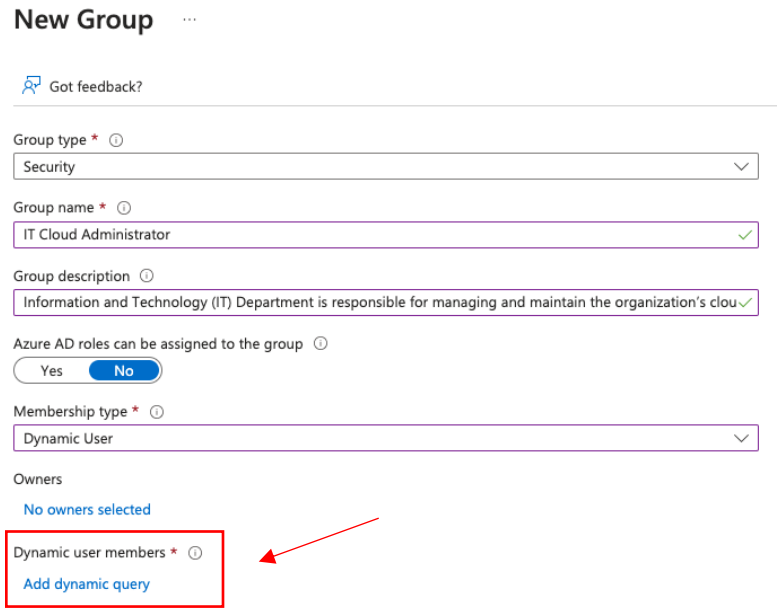
After the csv file has been uploaded successfully, you refresh the user management page to display the users in the Azure Active Directory for Contoso HealthCare.

Step 4: Return to the *Azure Active Directory* home page to create groups within the Azure AD. Under *manage*, select "**Groups**" follow by "**New group.**"



Fill out the "**New Group**" fields information with the department information. An example for the Information Technology department will be the following information:

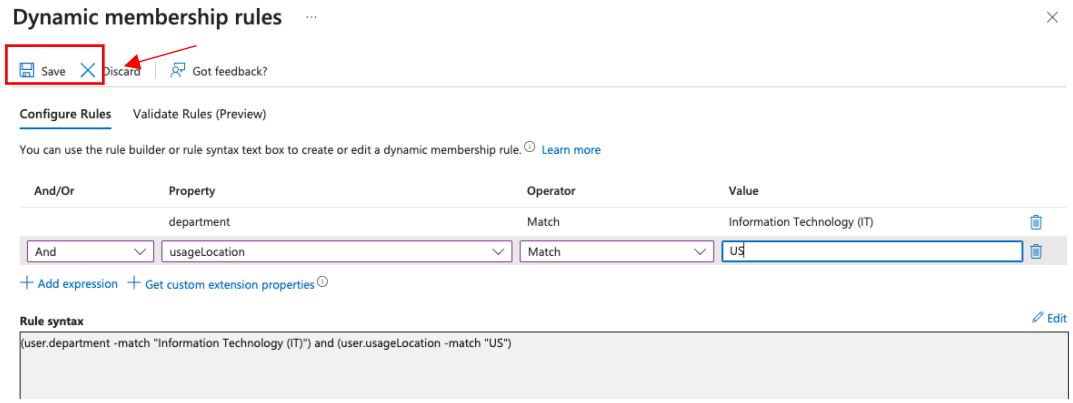
> **Group type:** Security
> **Group name:** IT Cloud Administrator
> **Group description:** Information and Technology (IT) Department is responsible for managing and maintain the organization's cloud infrastructure and services.
> **Membership type:** Dynamic User



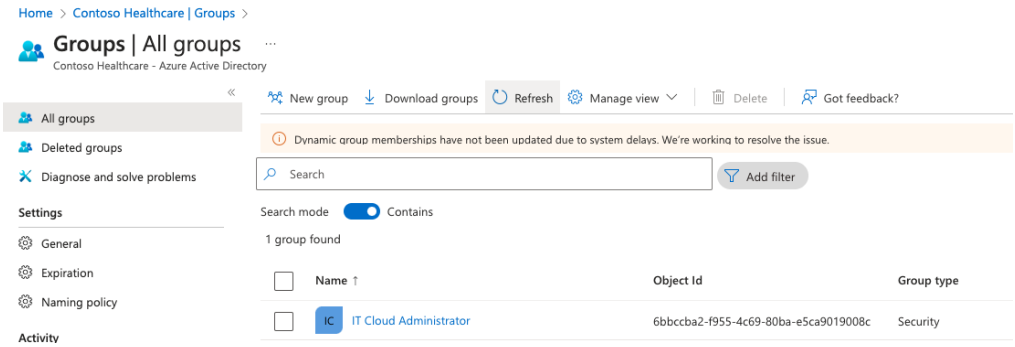
Select the "**Add dynamic query**" and fill out the dynamic membership rules for the IT Cloud Administrator Group.

Configure Rules are the following:

	Property: department	**Operator:** Match	**Value:** Information Technology (IT)
And	**Property:** usagelocation	**Operator:** Match	**Value:** US

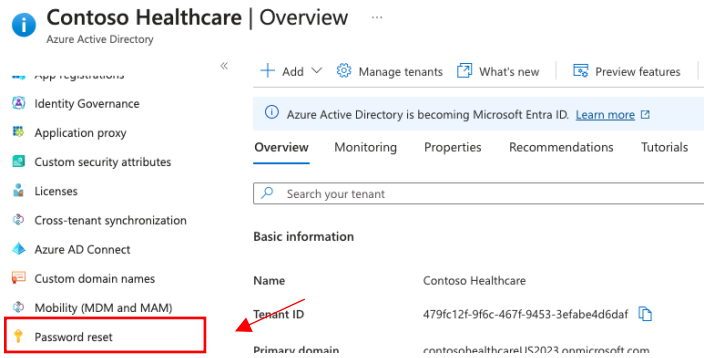


Select "**Save**" and "**Create**" the IT Cloud Administrator group.

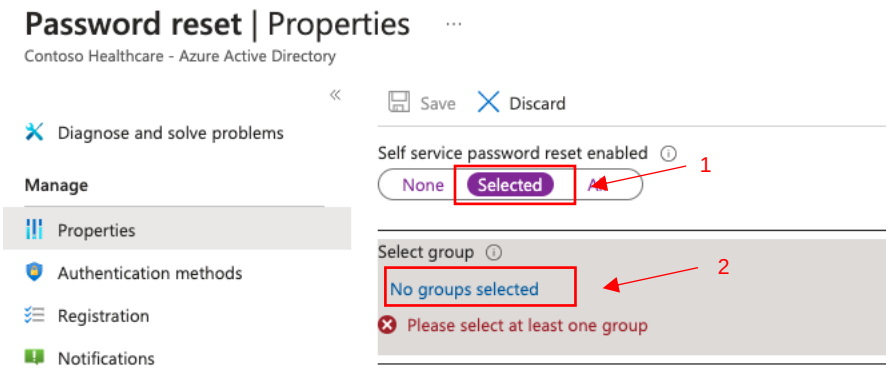


Note: I will apply the same steps to create the rest of the groups within Contoso Healthcare such as Finance and Account, Marketing and Communications Group etc

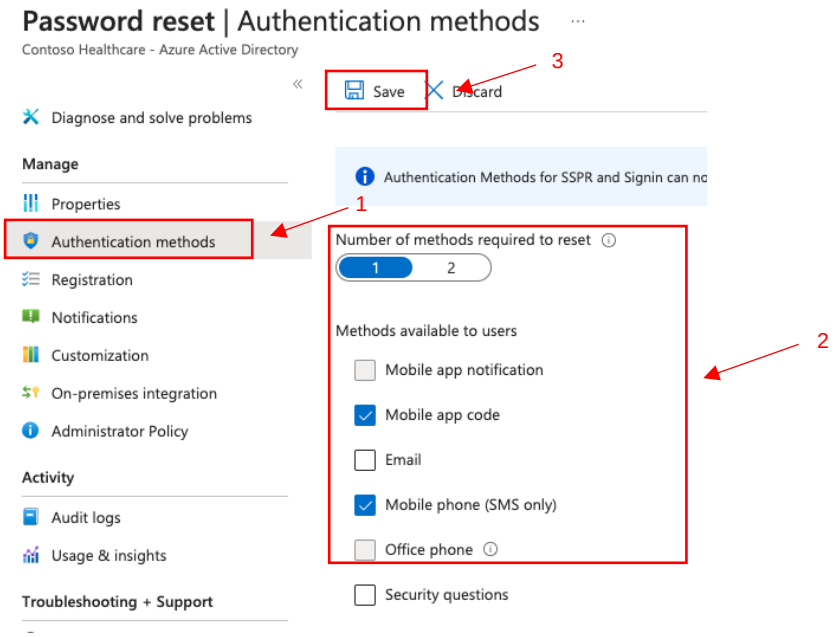
Step 5: Under *manage* in *Contoso Healthcare* | *Overview* select "**Password reset**" to configure the self-service password reset.



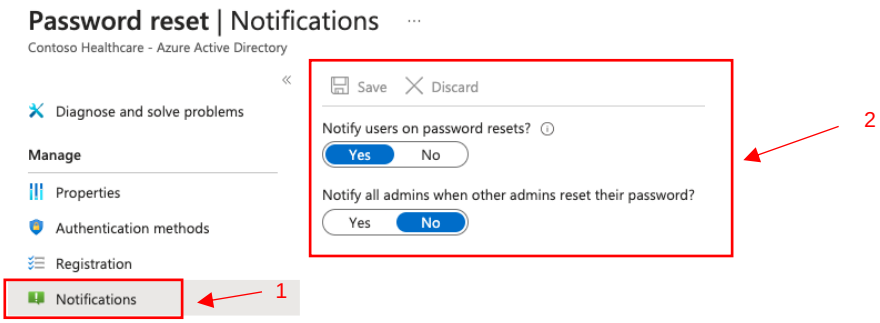
Under *self-service password reset enabled,* click on "**Selected**" and then select "**No groups selected**" to add the IT Cloud Administrator group to the password reset properties and "**Save.**"



We still need to applied authentication methods to ensure security to the self-service password reset. Select "**Authentication methods**", follow by selecting the "**Number of methods**" and the required authentication methods and select "**Save**".



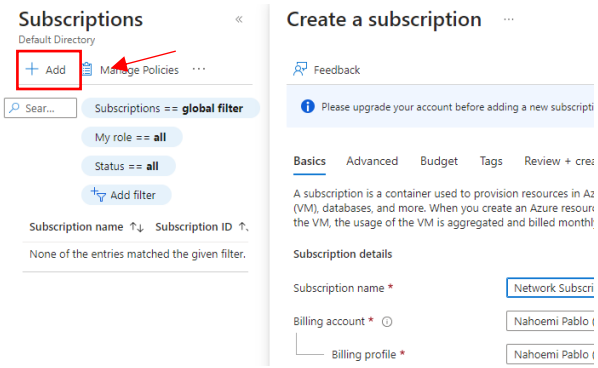
To add an additional layer of security, I would configure the password reset notification. Select "**Notifications**" and select "**Yes**" to notify users on password resets and "**No**" to notify the admin of this change.



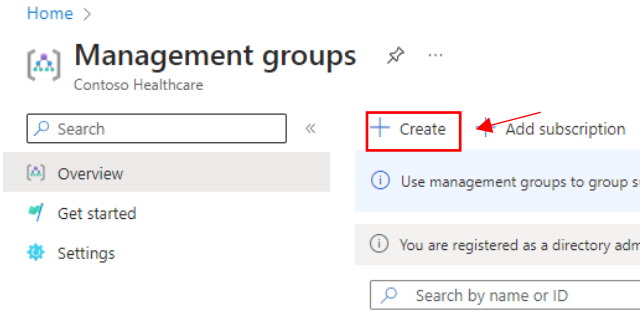
Part 2: Implement Azure role-based access controls (RBAC) by creating roles with appropriate permissions to Azure resource groups. Assign permissions to users and/or groups at the appropriate scopes to grant least privilege access.

The objective of the second phase involves creating and assigning Azure roles with specific permissions to users and groups based on their responsibilities.

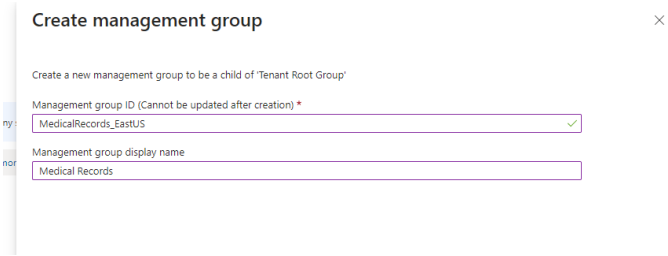
Step 1: To configure *subscription*, we start by searching for "**Subscriptions.**" In subscription select "**+ Add**" then fill up the subscription information and select "**Review + create**"



Step 2: To configure *Management Group* we start by searching for "**Management Group**." In management group select "**Create**" to develop a new management group to be a child management group of the "Tenant Root Group"

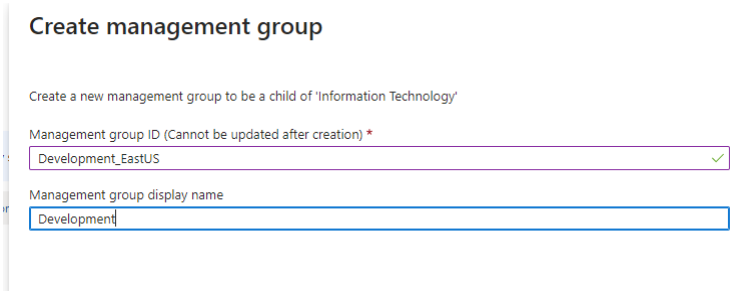


Fill out the management group information according to the Azure Management Diagram. Applied the same step for each management group in the diagram.

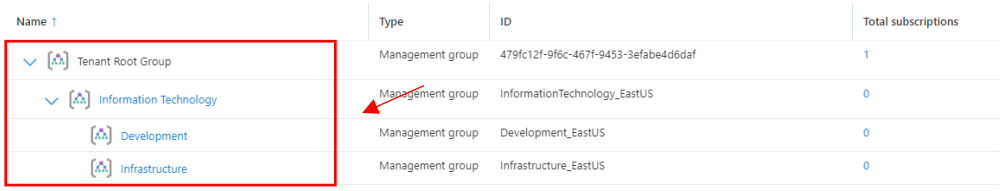


For illustration, I will continue to develop the management group for Information Technology. The Information Technology management group has two child groups: Development and Infrastructure. Select "**…**" and then "**+ Create child group here**" repeat this step to create both child groups.

Fill out the information for the child of "**Information Technology**" management group and "**Submit**."



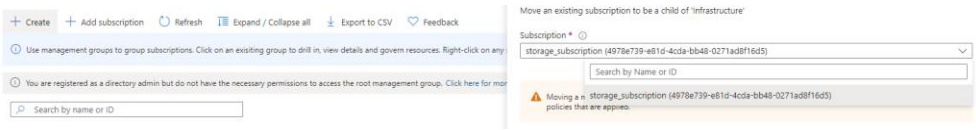
By pressing the refresh button, the new management groups will appear under their parent group(s). See below illustration.



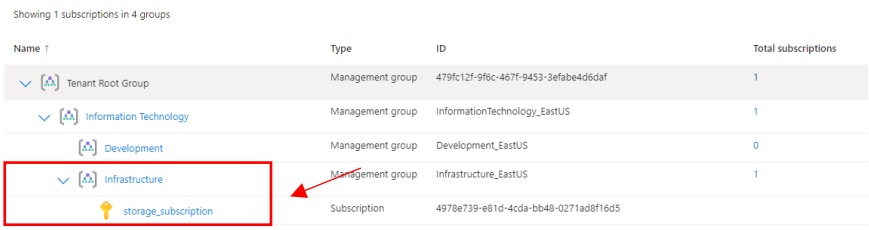
To finalize configuring the management groups in Contoso Healthcare, we need to add the subscription to each management group within the organization. The management group "Infrastructure" has three subscriptions: Networking Sub, Storage Sub, and Servers Sub. Let's configure the subscriptions for "Infrastructure" management group.

Step 3: At the infrastructure management group level, select "**…**" then "**+ add subscription here**."

In the new window, select the subscription name and select "**Save**".



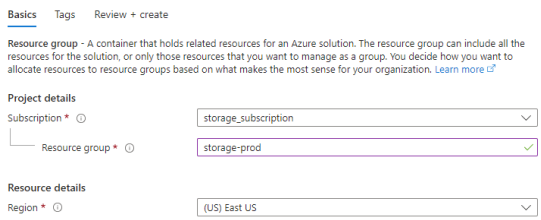
By pressing the refresh button, the subscription will appear under their parent group(s). See below illustration.



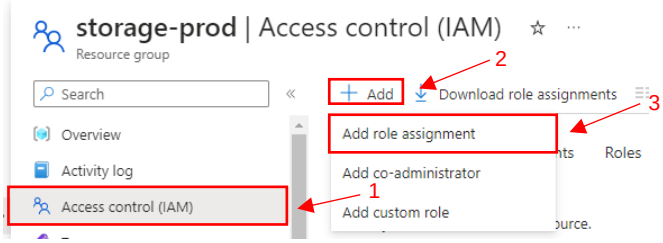
Step 4: Develop *resource groups* by searching for "**Resource groups**." In resource group select "**Create**" to develop a new resource group. Fill out the resource group page with the following information:

> **Subscription:** storage_subscription
> **Resource group:** storage-prod
> **Region:** (US) East US

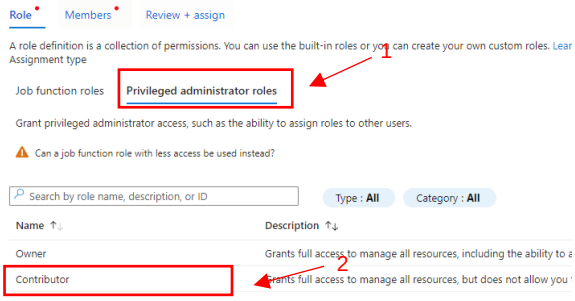
Leave tags blank for now and follow by "**Review + create**" then "**Create.**"



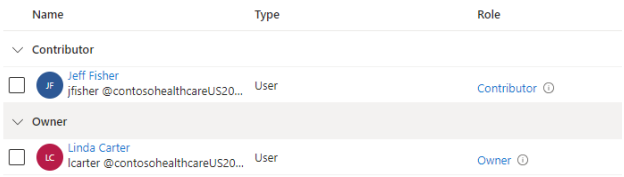
Step 5: In the resource group named "**Storage-prod**" select "**Access control (IAM)**" follow by "**+ Add**" and select "**add role assignment.**"



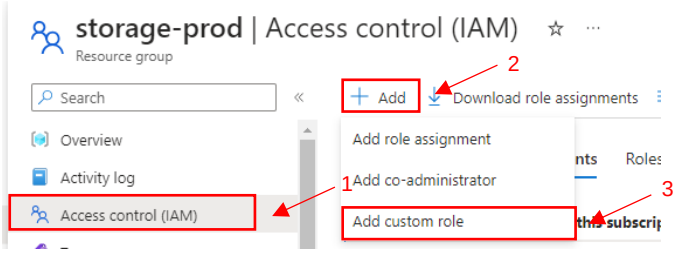
Step 6: In the *Access control (IAM) page*, select "**Privileged administrator roles**" and choose the role needed for the employee. For this project, we will select "**Contributor**."



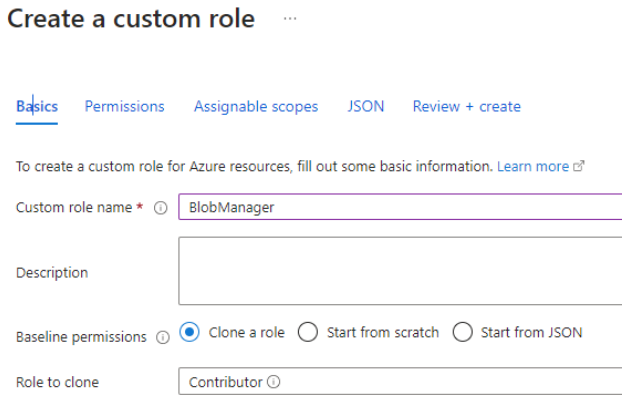
In the member tab, we select "**+ select members**", select the member and "**Review + assign**." For the storage-prod resource group we have an owner and a contributor.



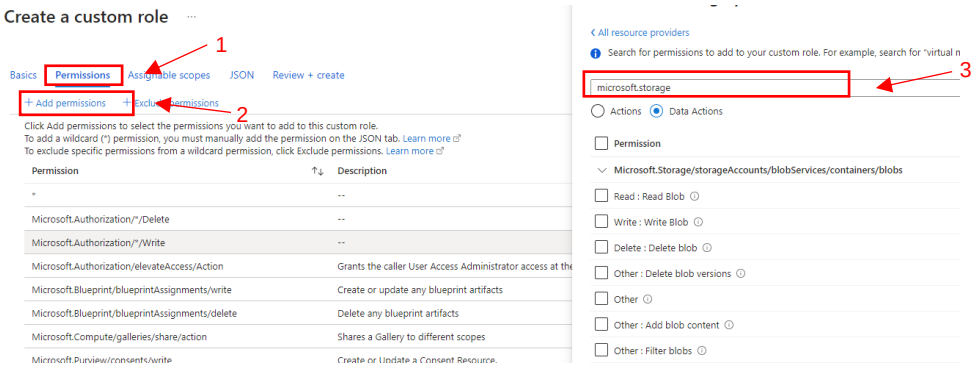
Step 7: To create a custom role, in resource group named "**Storage-prod**" select "**Access control (IAM)**" follow by "**+ Add**" and select "**add custom role.**"



In the "**Create a custom role**" page fill out the information.



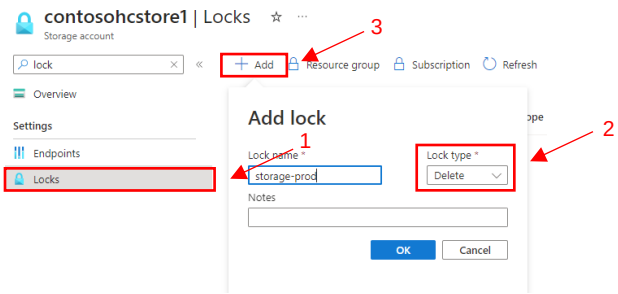
Review the *permission* tab then select "**+ Add permission**." Search "**Microsoft.storage**" and review/select the "**Actions**' and/or "**Data Actions**" you would like to add to the role.



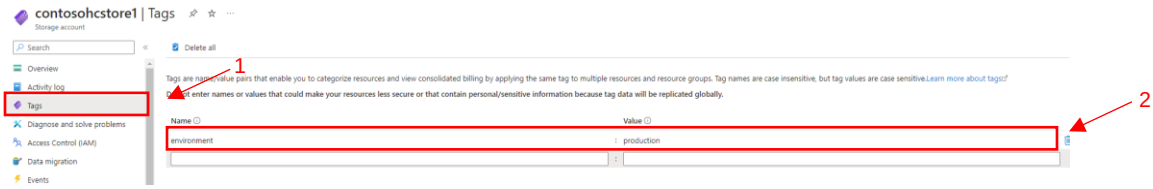
Part 3: Deploying governance tools such as Azure Policy, resource locks, and tags in the environment.

The purpose of Part 3 is implementing governance controls in the environment through Azure Policy, resource locking, and tagging strategies. This provides organizational guardrails and resource consistency through policies, locks to restrict changes, and metadata tags.

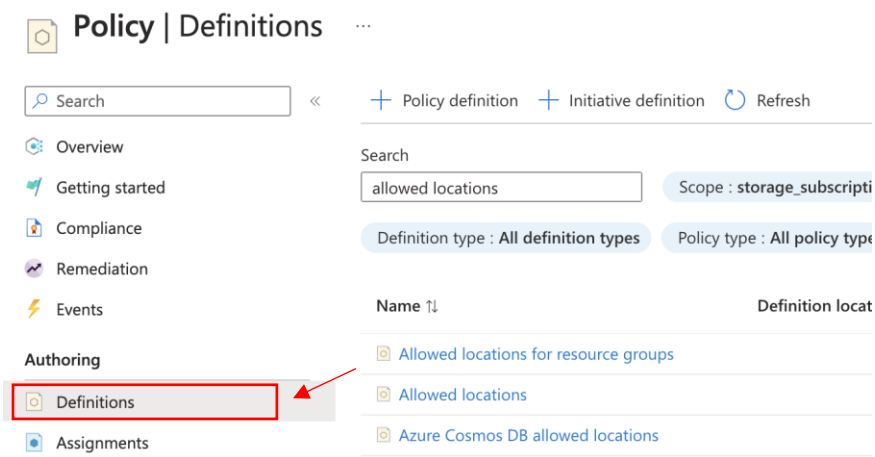
Step 1: In your resource, in this case "**contosohcstore1**" which is a storage account in "**storage-prod**" resource group. Search or scroll for "**Locks**" then select "**+ Add**" and fill out the "**lock name**". Change lock type to "**Delete**" to prevent accidental deletes.



Step 2: In "**contosohcstore1**" search or scroll for "**Tags**" and fill out the tag name and value follow by apply.

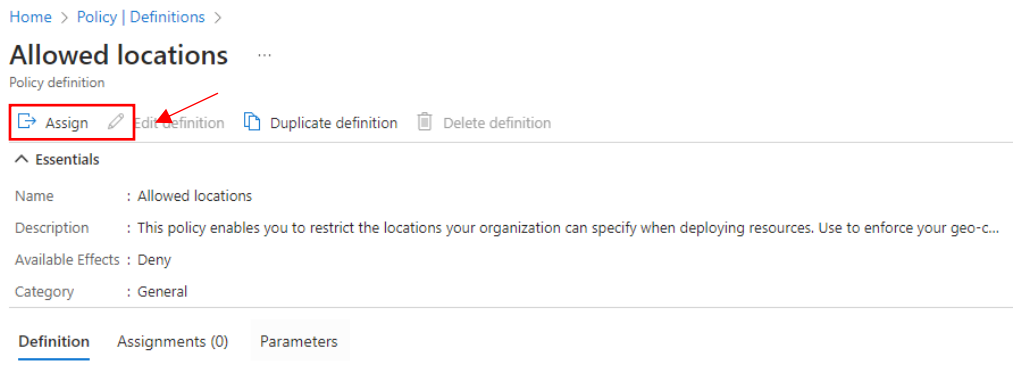


Step 3: Search for "**Policy.**" In *Policy overview page*, select "**Definitions**" then filter the list to find "**Location**" and select "**Allowed locations.**"

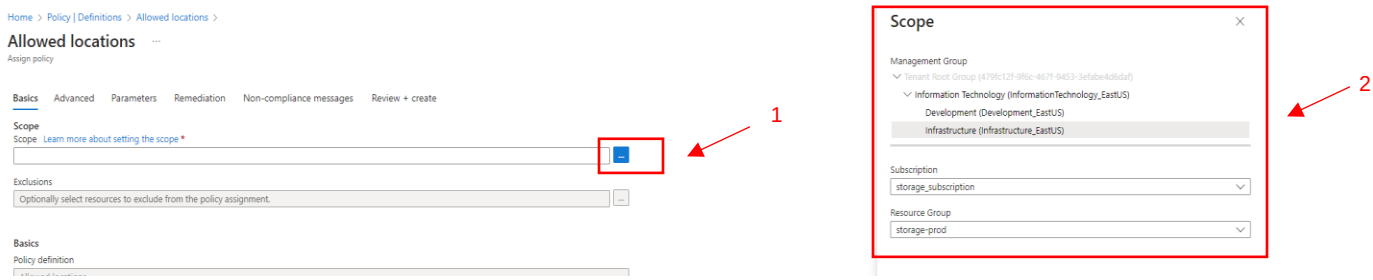


Note: This policy will allow resources to be deployed in a specific location.

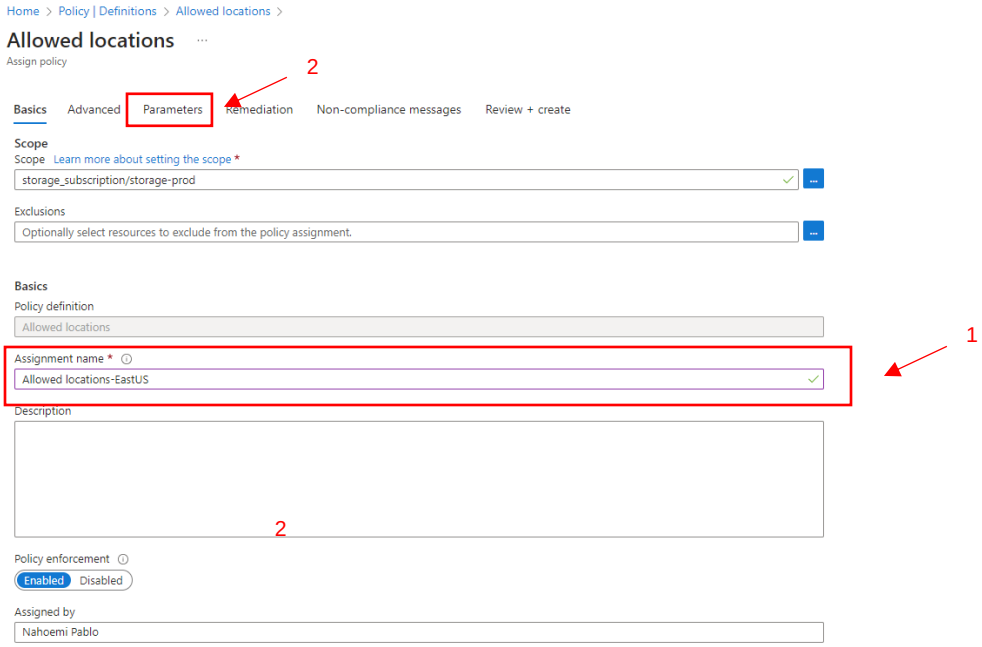
After locating the policy, select "**Assign**."



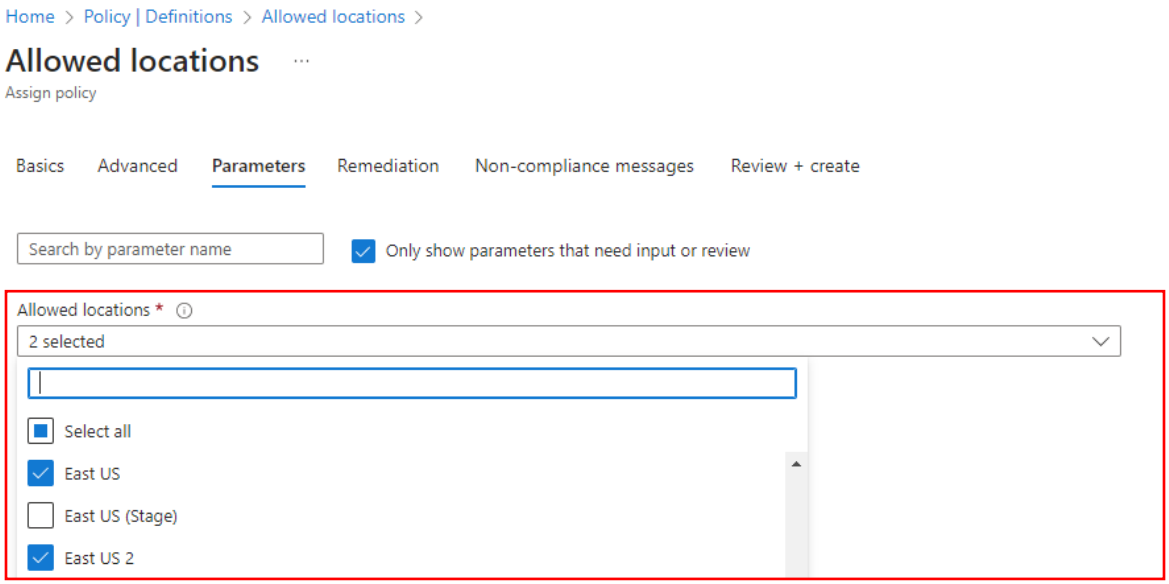
The next step in **Step 3** is to select "**…**" and choose the scope of the policy on the appropriate level such as Management Group, Subscription or Resource Group level and "**Select.**"



Modify the *Assignment name* to "**Allowed locations-EastUS**" and leave everything else to default then click "**Next**" to the "**Parameters**" tab.



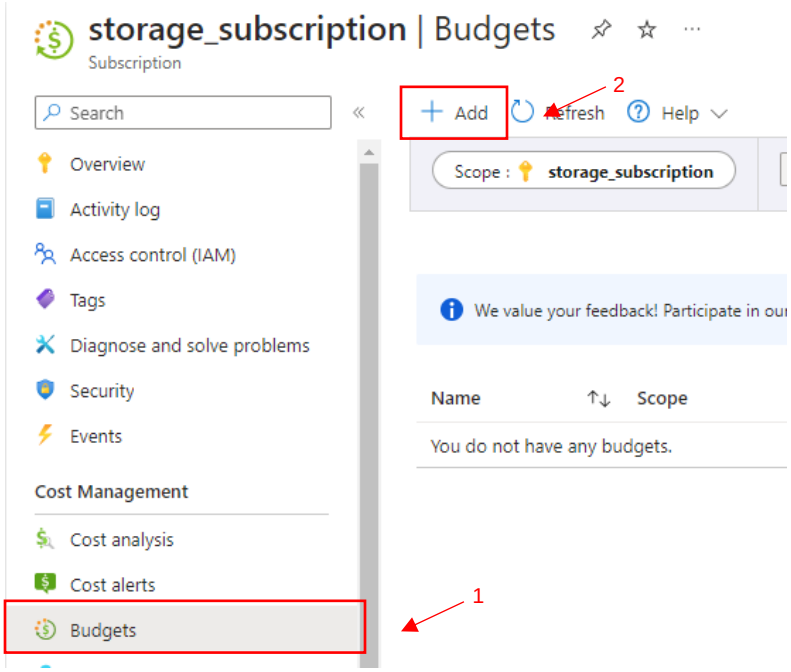
In the *parameters* tab select "**Allowed locations**" then choose "**East US**" and "**East US 2**" which are the locations that we are currently using for this project. Last, select "**Review + create.**"



Part 4: Optimize cost management through budgets, alerts, and advisors to maximize value while minimizing expense.

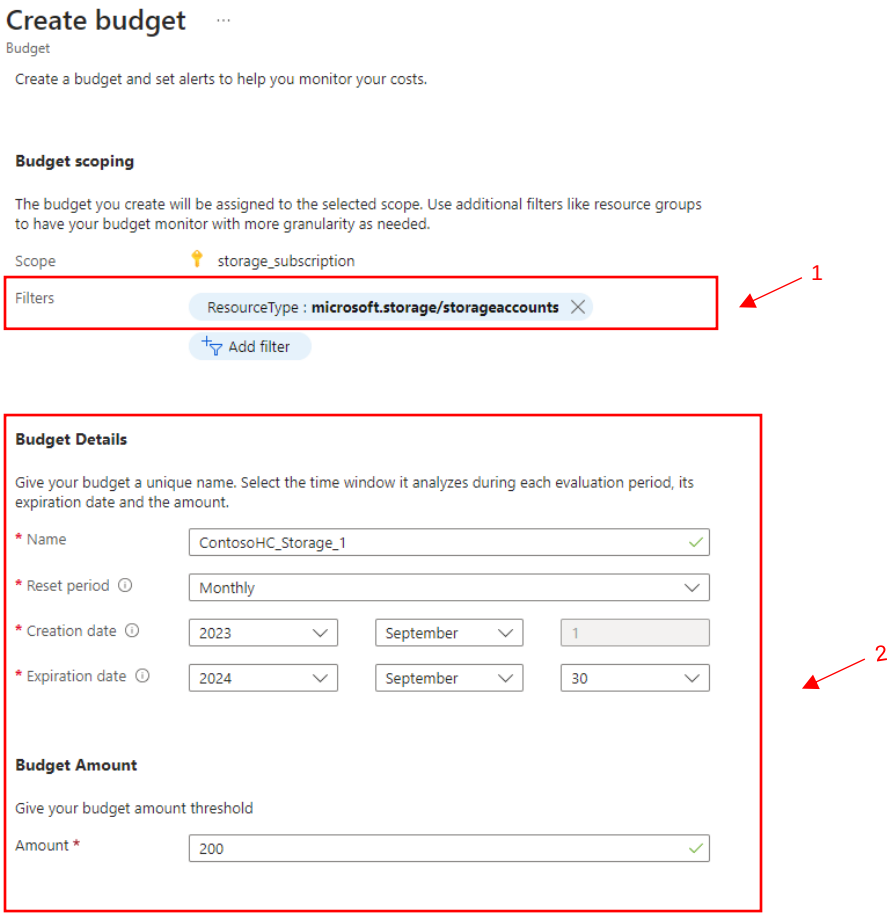
The aim of part four is to optimize cloud expenditures through budgets, alerts, and utilization reporting. This enables proactive cost management through monitoring, and visibility.

Step 1: In *subscription* overview page, select "**Budgets**" then "**+ Add**" setup budget and create alerts.



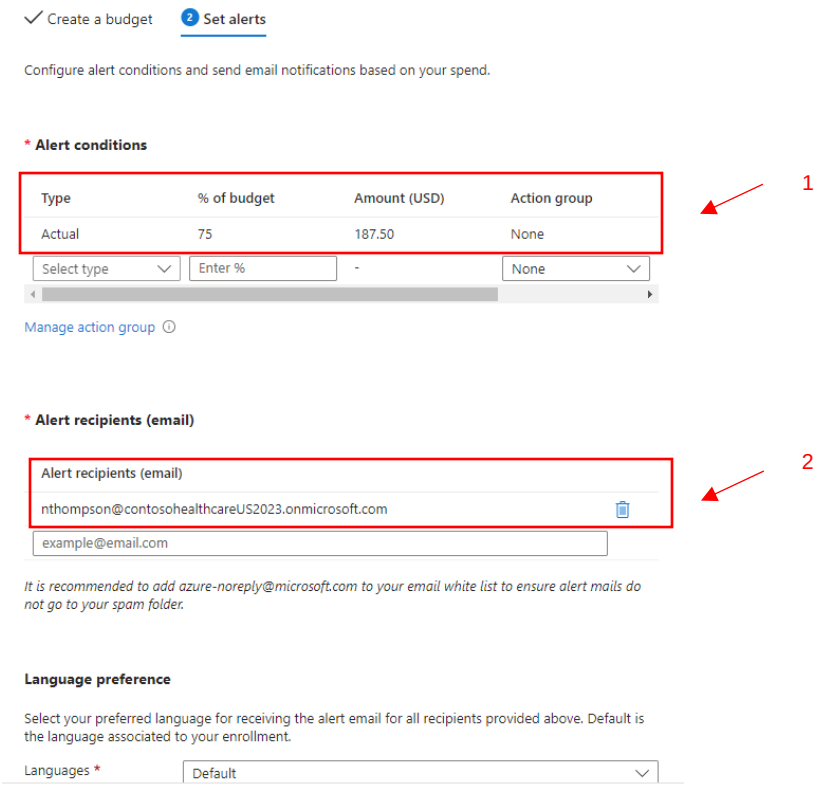
In the *Create budget* page, fill out the budget details, budget amount information then select "**Next**" to "**Set alerts**"

> **Name:** ContosoHC_Storage_1
> **Reset period:** Monthly
> **Creation date:** 2023, September 1
> **Expiration date:** 2024, September 30
> **Amount:** 200



Note: I use the filters for a granularity budget scoping for my resources.

Step 2: In the *Set alerts* page, select the type of condition "**Actual**", percent of the budget "**75**" which will display the amount of the budget. For the alert recipients, I will add the "**IT Manager email**" and select "**Create.**"



In conclusion, this project enabled comprehensive identity and access management for Contoso Healthcare within their Azure environment per cloud security best practices. Critical activities were undertaken including configuration of core Azure AD services for user identity and authentication, implementing least privilege access with Azure RBAC, enforcing organizational standards through centralized policies, and optimizing cost management.